ZILKA-KOTAB
PC
ZILKA, KOTAB & FEECE™

95 SOUTH MARKET ST., SUITE 420
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

Date:	July 7, 2005	**Phone Number**	**Fax Number**
To:	Examiner David Cervetti		(703) 872-9306
From:	Kevin J. Zilka		

Docket No.: NA11P011/01.116.01 **App. No: 09/895,508**

Total Number of Pages Being Transmitted, Including Cover Sheet: 34

Message:

Please deliver to Examiner David Cervetti.

Thank you,

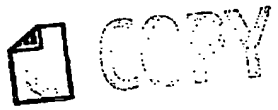
Kevin J. Zilka

☑ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

Practitioner's Docket No. NAI1P011/01.116.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: James S. Magdych et al.



Application No.: 09/895,508 Group No.: 2136
Filed: 06/29/2001 Examiner: Cervetti, D.
For: NETWORK-BASED RISK-ASSESSMENT TOOL FOR REMOTELY DETECTING LOCAL COMPUTER VULNERABILITIES

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION–37 C.F.R. § 41.37)

1. Transmitted herewith, in triplicate, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on May 13, 2005.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*
*(When using Express Mail, the Express Mail label number is **mandatory**;*
Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
_ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
_ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ (mandatory)

TRANSMISSION

✓ _ facsimile transmitted to the Patent and Trademark Office, (703) 872-9306.

Signature

Date: 7/7/2005

Erica [illegible] BBONNER 00000039 501351 09895508

(type or print name of person certifying) DA

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$500.00
Appeal Brief fee due	**$500.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R.1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$500.00
Extension fee (if any)	$0.00
TOTAL FEE DUE	**$500.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of $500.00 to Deposit Account No. 50-1351 (Order No. NAI1P011).

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P011).

Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of	
Magdych et al.	Group Art Unit: 2136
Application No. 09/895,508	Examiner: Cervetti, David
Filed: 6/29/2001	Docket No. NAI1P011_01.116.01
For: NETWORK-BASED RISK-ASSESSMENT TOOL FOR REMOTELY DETECTING LOCAL COMPUTER VULNERABILITIES	Date: July 7, 2005

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on May 13, 2005.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS

V SUMMARY OF CLAIMED SUBJECT MATTER

VI ISSUES

VII ARGUMENTS

VIII APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE APPELLANT IN THE APPEAL

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c)(1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

Since no such proceedings exist, no Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1, 4-6, 9-12, 15-17 and 20-35

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1, 4-6, 9-12, 15-17 and 20-35
3. Claims allowed: None
4. Claims rejected: 1, 4-6, 9-12, 15-17 and 20-35

C. CLAIMS ON APPEAL

The claims on appeal are: 1, 4-6, 9-12, 15-17 and 20-35

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, no such amendments exist.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1 et al., a method of remotely detecting vulnerabilities on a local computer is provided including installing an agent on a local computer (e.g. item 102 of Figure 1). Then, encrypted commands are received for executing a risk-assessment scan from a remote computer utilizing a network (e.g. item 104 of Figure 1). The commands on the local computer are decrypted utilizing the agent (e.g. item 106 of Figure 1) and are also processed on the local computer utilizing the agent (e.g. item 108 of Figure 1). The risk-assessment scan is then performed on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer (e.g. item 110 of Figure 1). In addition, the agent includes a plurality of risk-assessment modules (e.g. items 402 and 404 of Figure 4). The commands execute the risk-assessment modules in a specific manner that is configured at the remote computer and each indicate at least one of the risk-assessment modules. Further, the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters. Note page 6, lines 10-20; page 12, line 4-8; and page 13, lines 10-15, for example.

VI ISSUES (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1, 12 and 23-27 under 35 U.S.C. 112, second paragraph, as being indefinite.

Issue # 2: The Examiner has rejected Claims 1, 4-6, 9-10, 12, 15-17, 20-21 and 23-35 under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. (U.S. Patent No. 6,298,445) in view of Orchier et al. (U.S. Patent No. 6,070,244).

Issue #3: The Examiner has rejected Claims 11 and 22 under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. (U.S. Patent No. 6,298,445) in view of Orchier et al. (U.S. Patent No. 6,070,244) and in further view of Smid et al. (U.S. Patent No. 4,386,233).

VII ARGUMENTS (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue #1:

Issue # 1: The Examiner has rejected Claims 1, 12 and 23-27 under 35 U.S.C. 112, second paragraph, as being indefinite.

Group #1: Claims 1, 12 and 23-27

Specifically, the Examiner has stated that in the following claim limitations, it is unclear what is configured, the module or the execution of the modules:

> "wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer;"
>
> "wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters."

Appellant respectfully asserts that the above claim limitations clearly state that "the commands execute the risk-assessment modules in a specific manner that is configured," (emphasis added) and thus it is the manner of execution of the modules that is configured.

Issue #2:

The Examiner has rejected Claims 1, 4-6, 9-10, 12, 15-17, 20-21 and 23-35 under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. (U.S. Patent No. 6,298,445) in view of Orchier et al. (U.S. Patent No. 6,070,244).

Group #1: Claims 1, 6, 9-10, 12, 17, 20-21, 23-30, and 32

With respect to independent Claim 1, the Examiner has relied on the following excerpt from Shostack to meet appellant's claimed "wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer."

> "The network scan for IP devices is invoked using the properties (PROP) icon 72 which **enables an authorized local user 6 to configure** the various modules." (Col. 12, lines 55-57) (emphasis added)

Appellant respectfully asserts that the above excerpt from Shostack clearly *teaches away* from appellant's claim language by disclosing a properties icon that "enables an authorized local user to configure the various modules." Appellant, on the other hand, claims that the "commands execute the risk-assessment modules in a specific manner that is configured at the remote computer."

Furthermore, the Examiner has relied on the following excerpt from Orchier to make a prior art showing of appellant's claimed, "wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters."

> "The manual maintenance agent 86 takes inputs from the user and converts them into platform independent security maintenance instructions which are then processed by the maintenance agent abstraction facility 90. Examples of platform independent security maintenance categories and data are as follows:
> AddUserAccount(id, platformList, name, Payroll Number, expenseCode)
> RemoveUserAccount(id, platformList)

```
AddUserAccountToGroup(id, platformList, GroupName)
RemoveUserAccountFromGroup(id, platformList, GroupName)
ModifyUserAccountName(id, platformList, name)
ModifyUserAccountPay(id, platformList, Pay)
ModifyUserAccountExpenseCode(id, platformList, expenseCode)
DisableUserAccount(id, platformList)
```

FIG. 8c shows the screen used to designate how often data should be collected. FIG. 8d shows the screen used to designate the server from which data should be collected. FIG. 8e shows the screen used to designate high risk applications. FIG. 8f shows the screen used to designate the environment. FIG. 8g shows the screen used to designate high risk reports. FIG. 8h shows the screen used to designate event code mapping of native codes to the common system code." (Col. 14, lines 25-52)

Appellant respectfully asserts that the above excerpt from Orchier suggests taking inputs from a user regarding user accounts (see exemplary categories and data in above excerpt) and then converting those inputs into instructions to be processed by a maintenance agent. Thus, Orchier's user inputs regarding user accounts simply fail to meet appellant's "commands [that] are processed by extracting parameters...and executing the risk-assessment modules...utilizing the associated parameters. To emphasize, simply nowhere in Orchier is there any suggestion of "extracting parameters" or utilizing such parameters in "executing the risk-assessment modules," as claimed by appellant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claims 4 and 15

With respect to the present grouping, the Examiner relies on the following excerpt from Orchier to meet appellant's claimed "wherein the risk-assessment modules are selected for the agent based on specifications of the local computer" (see Claim 4 et al.).

> "The security domains 70a-70n communicate with collection agents 72a, 72b, 72c . . . 72n, respectively. These collection agents 72a-72n, a part of security administration system 50, represent software facilities written specifically for the corresponding operating system or system software components, for example the workstation server, LAN or NetWare.TM. software facility comprising the security domains 70a-70n. Therefore, there are many different collection agents, each of which is associated with a specific security domain type. The present invention has been reduced to practice with collection agents specific to Netware.TM. 3.1, NetWare.TM. 4.0, Windows NT, two different remote access servers, RACF, ACF2, Sybase, Oracle, AS 400, VAX/VMS, Tandem, Lotus Notes, four different UNIX operating systems and an Internet firewall.
>
> The collection agents 72a-72n use system utilities and/or APIs (Application Programming Interfaces) to extract from the individual security domains 70a-70n specific data defining security information pertaining to the system users, passwords, security groups, and where applicable: permissions, access controllers, logon events, file access events, system management events, file attributes, software and hardware versions, password control parameters, system parameters and the like. The information they collect is passed to the collection agent abstraction layer or facility 74 for further processing." (Col. 4, line 48-Col. 5, line 6 - emphasis added)

After carefully reviewing such excerpt and the remaining Orchier reference, however, it is clear that Orchier merely suggests security domains with collection agents each written for a specific domain type. Appellant notes, however, that Orchier also states that the collected data is analyzed to determine if user and system data comply with security policy requirements (Col. 7, lines 37-39). Thus, a specific collection agent is chosen according to the type of data to be collected. Choosing a collection agent for collecting data in order to further determine whether user and system data comply with security policy requirements, as taught in Orchier, simply fails to meet selecting "risk-assessment modules...based on specifications of the local compute," as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #3: Claims 5 and 16

third module...compare[s] and identif[ies] vulnerable passwords" (Col. 12, lines 61-63). Thus, it is clear that there is no mention or suggestion in Shostack of a STAT, READ, READDIR, FIND, and/or GETGRENT module, as required by appellant's claims.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #4: Claim 34

The Examiner has relied on the following excerpt from Shostack to make a prior art showing of appellant's claimed "wherein a plurality of the commands are each associated with only one of the risk-assessment modules."

> "Referring to FIGS. 5 and 6, the various integrated security system modules 160 are represented by corresponding symbols on a graphical user interface (GUI) screen 70. **The first module 74 is used to check the operating system.** The check is invoked by using the check operating systems 74' icon on the GUI screen. The **check involves ascertaining whether a user has the correct permission requirements to gain access to the network.** Also, in one embodiment of the invention, **the first module 74 determines whether all known vulnerabilities have been addressed.** Specifically, the first module 74 determines whether the suggested changes resulting from the installation procedure (Step 118) have been made to the operating system." (Col. 12, lines 14-26-emphasis added)

First, appellant respectfully asserts that the above excerpt merely teaches "a first module," and not multiple "risk-assessment modules," as claimed by appellant. In addition, Shostack simply discloses a first module that checks an operating system, in which it is determined whether a user has correct permission to gain access to a network, and that determines whether all known vulnerabilities have been addressed (see emphasized excerpt above). Merely checking to make sure vulnerabilities have been addressed clearly does not meet appellant's claimed "plurality of the commands [that] are each associated with only one of the risk-assessment modules,"

since, in the above excerpt from Shostack, there is no mention of commands, in the context claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #5: Claim 31

With respect to dependent Claim 31, the Examiner has relied on the following excerpt from Shostack to make prior art showing of appellant's claimed "wherein the feedback includes descriptions as to how to correct the vulnerabilities.

> "The present invention provides such a mechanism by **automatically providing enhancements to a database of security vulnerabilities and using that information to provide security solutions** to potentially "weak" computer networks and/or computers." (Col. 4, lines 8-12 - emphasis added)
>
> "The GUI 70 may also provide a reporting mechanism. The GUI 70 may also include several means for reporting various network transactions. In the disclosed invention, the GUI 70 includes a log view 80 may allow a user to view a text version the update process or log information on a storage device, a log update 82 that generates a report of all security vulnerabilities on the network 20, and a log clear function 84 that allows a user to erase the log." (col. 13, lines 36-44)

Appellant respectfully disagrees. In the above cited excerpts as relied on by the Examiner, Shostack teaches automatically providing enhancements and providing security solutions to vulnerable computers. The only reporting Shostack discloses relates to logs of an update process, storage device, and security vulnerabilities. Thus, Shostack suggests automatically providing enhancements and solutions to security vulnerabilities without ever giving descriptions on how to correct the vulnerabilities. For these reasons, the Shostack reference clearly fails to meet appellant's claimed "wherein the feedback includes descriptions as to how to correct the vulnerabilities."

In the advisory action dated April 29, 2005, the Examiner responds by stating that Table 1 in Columns 5-6 shows information regarding the vulnerabilities is in the database.

Appellant respectfully asserts that the database the Examiner relies on simply includes descriptions on what vulnerabilities to check for with respect to different types of network features. For example, the database states that for a firewall, "check the firewall for vulnerability to routing, IP spoofing, and other attacks" (see specifically Col. 5, line 59). Thus, clearly the database disclosed in Shostack does not teach "feedback [that] includes descriptions as to how to correct the vulnerabilities," as claimed by appellant.

Yet again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #6: Claim 35

With respect to dependent Claim 35, the Examiner has rejected such claim limitations based on col. 4, lines 48-62 of Orchier. Appellant respectfully asserts that the Orchier reference fails to meet appellant's claimed technique "wherein a different set of risk-assessment modules exist on different local computers, based on a platform associated with each of the local computers."

In the advisory action dated April 29, 2005, the Examiner responds by stating "Orchier teaches collection agents specific to different platforms (Netware, Windows, 4 different UNIX operating systems, etc.)."

Again, appellant respectfully asserts that after carefully reviewing such excerpt and the remaining Orchier reference, however, it is clear that Orchier merely suggests security domains with collection agents each written for a specific domain type.

Appellant notes, however, that Orchier also states that the collected data is analyzed to determine if user and system data complies with security policy requirements (Col. 7, lines 37-39). Thus, a specific collection agent is chosen according to the type of data to be collected. Choosing a collection agent for collecting data in order to further determine whether user and system data complies with security policy requirements, as taught in Orchier, simply fails to meet selecting "a different set of risk-assessment modules [that] exist on different local computers, based on a platform associated with each of the local computers," as claimed by appellant (emphasis added).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue #3

The Examiner has rejected Claims 11 and 22 under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. (U.S. Patent No. 6,298,445) in view of Orchier et al. (U.S. Patent No. 6,070,244) and in further view of Smid et al.(U.S. Patent No. 4,386,233).

Group #1: Claims 11 and 22

The Examiner has relied on the following excerpt from Smid to make a prior art showing of appellant's claimed technique "wherein commands are decrypted utilizing a shared key."

> "Alternatively, authentication is accomplished by controlling access to the cryptographic function by encrypting user commands with a cryptographic function using a password supplied by the user as the cryptographic key and then **decrypting the encrypted commands using a prestored version of the password as the cryptographic key.**" (Col. 3, lines 5-12 - emphasis added)

Appellant respectfully asserts that Smid teaches "decrypting the encrypted commands using a prestored version of the password," which fails to meet the specificity of appellant's utilization of a "shared key." It is noted that a prestored version of a password as a key does not meet appellant's claimed "shared key" since a prestored version of a password does not have any bearing on whether the key is shared.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII APPENDIX OF CLAIMS (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A method of remotely detecting vulnerabilities on a local computer, comprising:

a) installing an agent on a local computer;

b) receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network;

c) decrypting the commands on the local computer utilizing the agent;

d) processing the commands on the local computer utilizing the agent; and

e) performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer;

wherein the agent includes a plurality of risk-assessment modules;

wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer;

wherein the commands each indicate at least one of the risk-assessment modules;

wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters.

2. (Cancelled)

3. (Cancelled)

4. (Previously Presented) The method as recited in claim 1, wherein the risk-assessment modules are selected for the agent based on specifications of the local computer.

5. (Previously Presented) The method as recited in claim 1, wherein the risk-assessment modules include a STAT module for performing a stat system call on a file, a READ module for reading a file, a READDIR module for returning contents of a directory, a FIND module for locating a list of files based on a given function, a GETPWENT module for retrieving an entry from a password database, a GETGRENT module for retrieving an entry from a group database, a CHKSUM module for performing a checksum operation on a file, and an EXEC module for executing a command.

6. (Previously Presented) The method as recited in claim 1, wherein the risk-assessment modules are selected from the group consisting of a STAT module for performing a stat system call on a file, a READ module for reading a file, a READDIR module for returning contents of a directory, a FIND module for locating a list of files based on a given function, a GETPWENT module for retrieving an entry from a password database, a GETGRENT module for retrieving an entry from a group database, a CHKSUM module for performing a checksum operation on a file, and an EXEC module for executing a command.

7. (Cancelled)

8. (Cancelled)

9. (Original) The method as recited in claim 1, and further comprising transmitting results of the risk-assessment scan from the local computer to the remote computer utilizing the network.

10. (Original) The method as recited in claim 9, and further comprising receiving feedback to the results from the remote computer utilizing the network.

11. (Original) The method as recited in claim 1, wherein the commands are decrypted utilizing a shared key.

12. (Previously Presented) A computer program product embodied on a computer readable medium for remotely detecting vulnerabilities on a local computer, comprising:

a) computer code for installing an agent on a local computer;

b) computer code for receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network;

c) computer code for decrypting the commands on the local computer utilizing the agent;

d) computer code for processing the commands on the local computer utilizing the agent; and

e) computer code for performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer;

wherein the agent includes a plurality of risk-assessment modules;

wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer;

wherein the commands each indicate at least one of the risk-assessment modules;

wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters.

13. (Cancelled)

14. (Cancelled)

15. (Previously Presented) The computer program product as recited in claim 12, wherein the risk-assessment modules are selected for the agent based on specifications of the local computer.

16. (Previously Presented) The computer program product as recited in claim 12, wherein the risk-assessment modules include a STAT module for performing a stat system call on a file, a READ module for reading a file, a READDIR module for returning contents of a directory, a FIND module for locating a list of files based on a given function, a GETPWENT module for retrieving an entry from a password database, a GETGRENT module for retrieving an entry from a group database, a CHKSUM module for performing a checksum operation on a file, and an EXEC module for executing a command.

17. (Previously Presented) The computer program product as recited in claim 12, wherein the risk-assessment modules are selected from the group consisting of a STAT module for performing a stat system call on a file, a READ module for reading a file, a READDIR module for returning contents of a directory, a FIND module for locating a list of files based on a given function, a GETPWENT module for retrieving an entry from a password database, a GETGRENT module for retrieving an entry from a group database, a CHKSUM module for performing a checksum operation on a file, and an EXEC module for executing a command.

18. (Cancelled)

19. (Cancelled)

20. (Original) The computer program product as recited in claim 12, and further comprising computer code for transmitting results of the risk-assessment scan from the local computer to the remote computer utilizing the network.

21. (Original) The computer program product as recited in claim 20, and further comprising computer code for receiving feedback to the results from the remote computer utilizing the network.

22. (Original) The computer program product as recited in claim 12, wherein the commands are decrypted utilizing a shared key.

23. (Previously Presented) A system for remotely detecting vulnerabilities on a local computer, comprising:

a) an agent installed on a local computer for receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network, decrypting the commands on the local computer, and processing the commands on the local computer; and

b) wherein the risk-assessment scan is performed on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer;

wherein the agent includes a plurality of risk-assessment modules;

wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer;

wherein the commands each indicate at least one of the risk-assessment modules;

wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters.

24. (Previously Presented) A system for remotely detecting vulnerabilities on a local computer, comprising:

a) means for installing an agent on a local computer;

b) means for receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network;

c) means for decrypting the commands on the local computer utilizing the agent;

d) means for processing the commands on the local computer utilizing the agent; and

e) means for performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer;

wherein the agent includes a plurality of risk-assessment modules;

wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer;

wherein the commands each indicate at least one of the risk-assessment modules;

wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters.

25. (Previously Presented) A method of remotely detecting vulnerabilities from a remote computer, comprising:

a) sending encrypted commands from a remote computer to an agent on a local computer for executing a risk-assessment scan utilizing a network, the commands adapted for being decrypted and processed on the local computer utilizing the agent for performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer;

b) receiving results of the risk-assessment scan from the local computer utilizing the network; and

c) transmitting feedback to the results from the remote computer to the local computer utilizing the network;

wherein the agent includes a plurality of risk-assessment modules;

wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer;

wherein the commands each indicate at least one of the risk-assessment modules;

wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters.

26. (Previously Presented) A computer program product embodied on a computer readable medium for remotely detecting vulnerabilities from a remote computer, comprising:

a) computer code for sending encrypted commands from a remote computer to an agent on a local computer for executing a risk-assessment scan utilizing a network, the commands adapted for being decrypted and processed on the local computer utilizing the agent for performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer;

b) computer code for receiving results of the risk-assessment scan from the local computer utilizing the network; and

c) computer code for transmitting feedback to the results from the remote computer to the local computer utilizing the network;

wherein the agent includes a plurality of risk-assessment modules;

wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer;

wherein the commands each indicate at least one of the risk-assessment modules;

wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters.

27. (Previously Presented) A method of remotely detecting vulnerabilities on a local computer, comprising:

a) installing an agent on a local computer, the agent including a plurality of risk-assessment modules selected based on at least one aspect of the computer;

b) receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network;

c) decrypting the commands on the local computer utilizing the agent;

d) authenticating the commands on the local computer utilizing the agent;

e) processing the commands on the local computer utilizing the agent, the commands adapted to execute the risk-assessment modules in a specific manner that is configured at the remote computer;

f) performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer;

g) transmitting results of the risk-assessment scan from the local computer to the remote computer utilizing the network;

h) receiving feedback to the results from the remote computer utilizing the network;

wherein the commands each indicate at least one of the risk-assessment modules;

wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters.

28. (Previously Presented) The computer program product as recited in claim 10, wherein the feedback is active.

29. (Previously Presented) The computer program product as recited in claim 28, wherein the feedback includes additional commands and additional modules for correcting the vulnerabilities in response to the additional commands.

30. (Previously Presented) The computer program product as recited in claim 10, wherein the feedback is passive.

31. (Previously Presented) The computer program product as recited in claim 30, wherein the feedback includes descriptions as to how to correct the vulnerabilities.

32. (Previously Presented) The computer program product as recited in claim 9, wherein the results include a log of the risk-assessment scan.

33. (Previously Presented) The computer program product as recited in claim 32, wherein the results include an identification of the vulnerabilities.

34. (Previously Presented) The computer program product as recited in claim 1, wherein a plurality of the commands are each associated with only one of the risk-assessment modules.

35. (Previously Presented) The computer program product as recited in claim 1, wherein a different set of risk-assessment modules exists on different local computers, based on a platform associated with each of the local computers.

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE APPELLANT IN THE APPEAL (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P011_01.116.01).

Respectfully submitted,

By: _____ Date: 7/7/05

Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660